

*J. Symbolic Computation* (1996) **21**, 139–153

# Analogs of Gröbner Bases in Polynomial Rings over a Ring

J. LYN MILLER<sup>†</sup>*Department of Mathematics, Western Kentucky University, Bowling Green, KY 42101, USA**(Received 18 August 1994)*


---

In this paper we will define analogs of Gröbner bases for  $R$ -subalgebras and their ideals in a polynomial ring  $R[x_1, \dots, x_n]$  where  $R$  is a noetherian integral domain with multiplicative identity and in which we can determine ideal membership and compute syzygies. The main goal is to present and verify algorithms for constructing these Gröbner basis counterparts. As an application, we will produce a method for computing generators for the first syzygy module of a subset of an  $R$ -subalgebra of  $R[x_1, \dots, x_n]$  where each coordinate of each syzygy must be an element of the subalgebra.

© 1996 Academic Press Limited

## 1. Introduction

The concept of Gröbner bases (introduced by Buchberger (1965); see Buchberger (1985) also) for ideals of a polynomial ring over a field  $k$  can be adapted in a natural way for  $k$ -subalgebras of such a polynomial ring. Robbiano and Sweedler (1988) defined a SAGBI (Subalgebra Analog to Gröbner Bases for Ideals) basis for a  $k$ -subalgebra  $A$  of  $k[x_1, \dots, x_n]$  to be a subset  $F \subseteq A$  whose leading power products generate the multiplicative monoid of leading power products of  $A$ ; this concept was independently developed by Kapur and Madlener (1989). The properties and applications of SAGBI bases strongly imitate many of the standard Gröbner basis results (see the texts by Adams and Loustau (1994), Becker and Weispfennig (1993), and Cox, Little, and O'Shea (1992) for an overview of the standard theory) when a suitable accompanying reduction algorithm is defined. Sweedler (1988) went on to extend the theory of Gröbner bases in a way that can be used to define them for ideals of  $k$ -subalgebras of  $k[x_1, \dots, x_n]$ ; this was briefly presented more explicitly by Ollivier (1990). Based on their work, we define a SAGBI-Gröbner basis for an ideal  $I$  of a  $k$ -subalgebra  $A \subseteq k[x_1, \dots, x_n]$  to be a subset  $G \subseteq I$  whose leading power products generate the monoid-ideal consisting of the leading power products of  $I$  in the monoid of those of  $A$ . Basic properties and applications of SAGBI-Gröbner bases in  $k[x_1, \dots, x_n]$  are again straight-forward adaptations of the usual Gröbner basis theory (see also Miller (1994)).

Our aim in this paper is to extend the theory of SAGBI and SAGBI-Gröbner bases to the context of a polynomial ring over a noetherian integral domain  $R$  in which we can

<sup>†</sup> E-mail: [miller@pulsar.cs.wku.edu](mailto:miller@pulsar.cs.wku.edu)

determine ideal membership and compute syzygies. (This constructive setting also provides an instantiation of the general theory developed by Robbiano (1986) for Gröbner bases in graded structures.) As we know from the study of this same extension process for Gröbner bases (refer to Zacharias (1978), Möller (1989), or Trinks (1978)), the leading coefficients of the polynomials now play a large role. The definitions, results, and especially techniques in this new setting are no longer such carbon copies of those for Gröbner bases, although we always attempt to parallel them as much as possible. In particular, the definition of a SAGBI basis in  $R[x_1, \dots, x_n]$  must now allow for addition of leading terms, not just multiplication. Therefore, the monoid of leading power products used for SAGBI bases in  $k[x_1, \dots, x_n]$  must be exchanged for a much larger structure, namely, the  $R$ -subalgebra that this monoid generates in  $R[x_1, \dots, x_n]$ . Likewise, for SAGBI-Gröbner bases in  $R[x_1, \dots, x_n]$ , the monoid-ideal in the definition over  $k[x_1, \dots, x_n]$  must be enlarged to an ideal of the new  $R$ -subalgebra just mentioned.

The main goals of this paper are to present and verify algorithms for constructing SAGBI and SAGBI-Gröbner bases in  $R[x_1, \dots, x_n]$  and to outline some of their basic properties. As an application, we will also present a method for computing generators for the first syzygy module of a subset of an  $R$ -subalgebra of  $R[x_1, \dots, x_n]$  where each coordinate of each syzygy must be an element of the subalgebra.

## 2. Notation

Our context is the polynomial ring  $R[x_1, \dots, x_n]$  in  $n$  variables, where  $R$  is a noetherian integral domain in which we can determine ideal membership and compute syzygies. (When the coefficient ring is a field, we use the symbol  $k$  instead of  $R$ .) We abbreviate this polynomial ring as  $R[X]$ . The notation  $R[S]$  stands for the  $R$ -subalgebra generated by the subset  $S \subseteq R[X]$ . Throughout this paper,  $A$  is an  $R$ -subalgebra of  $R[X]$ .

The symbol  $\mathbf{N}$  represents the non-negative integers, and  $\mathbf{T}_X$  represents the set of all power products  $\prod_{i=1}^n x_i^{\beta_i}$  with  $\beta_i \in \mathbf{N}$  of the variables  $x_1, \dots, x_n$ . We will often abbreviate such a power product as  $X^{\vec{\beta}}$  where  $\vec{\beta}$  is the exponent vector  $(\beta_1, \dots, \beta_n)$ . More generally, we have

**DEFINITION 2.1.** Let  $S \subseteq R[X]$ . An  $S$ -power product is a (finite) product of the form  $s_1^{e_1} \cdots s_m^{e_m}$  where  $s_i \in S$  and  $e_i \in \mathbf{N}$  for  $1 \leq i \leq m$ . We usually write this simply as  $S^{\vec{e}}$ , where  $\vec{e}$  represents that vector in  $\oplus_S \mathbf{N}$  whose coordinates are all 0 except for  $e_1, \dots, e_m$  in the positions corresponding to  $s_1, \dots, s_m$ .

**DEFINITION 2.2.** Given a term order on  $R[X]$ ,  $p \in R[X]$ , and  $S \subseteq R[X]$ , we define

$$\begin{aligned} \text{lp}(p) &= \text{the leading } X\text{-power product of } p \\ \text{lc}(p) &= \text{the leading coefficient of } p \\ \text{lt}(p) &= \text{lc}(p)\text{lp}(p) = \text{the leading term of } p \\ \text{Lp}S &= \{\text{lp}(s) : s \in S\} \end{aligned}$$

while  $\text{Lc}S$  and  $\text{Lt}S$  are similarly defined. We also establish the convention that  $\text{lp}(0)$  is undefined while  $\text{lc}(0)$  and  $\text{lt}(0)$  are 0.

We borrow the following terminology from Robbiano and Sweedler (1988).

DEFINITION 2.3. Let  $S \subseteq R[X]$ . Given an expression  $\sum_{i=1}^N r_i s_i$  with  $r_i \in R$  and  $s_i \in S$ , we define its height, written  $\text{ht}(\sum_{i=1}^N r_i s_i)$ , to be  $\max_i \text{lp}(s_i)$ . Moreover, we say that  $s_{i_0}$  contributes to the height of the expression if  $\text{lp}(s_{i_0}) = \max_i \text{lp}(s_i)$ .

We emphasize that the height is defined only for specific representations of an element of  $R[X]$ , not for that element itself.

### 3. SAGBI Bases in $R[X]$

Our first goal is to define a SAGBI basis and present an algorithm for its construction.

DEFINITION 3.1. Let  $A$  be an  $R$ -subalgebra of  $R[X]$ . We say that  $F \subseteq A$  is a SAGBI basis for  $A$  if  $\text{Lt}F$  generates the  $R$ -subalgebra  $R[\text{Lt}A]$ , i.e.  $R[\text{Lt}A] = R[\text{Lt}F]$ .

We consider an operation which parallels the reduction algorithm used in Gröbner basis theory.

DEFINITION 3.2. Let  $g \in R[X]$ , and let  $F \subseteq R[X]$ . We will say that  $g$  s-reduces to  $h$  via  $F$  in one step, written  $g \xrightarrow{F} h$ , if there exist a non-zero term  $cX^{\vec{\beta}}$  of  $g$  and  $F$ -power products  $F^{\vec{e}_1}, \dots, F^{\vec{e}_N}$  such that

1.  $\text{lp}(F^{\vec{e}_i}) = X^{\vec{\beta}}$  for  $1 \leq i \leq N$ .
2.  $c = \sum_{i=1}^N r_i \text{lc}(F^{\vec{e}_i})$  for some  $r_i \in R$  for  $1 \leq i \leq N$ .
3.  $h = g - \sum_{i=1}^N r_i F^{\vec{e}_i}$ .

We also write  $g \xrightarrow{F} h$  if there is a finite chain of 1-step s-reductions leading from  $g$  to  $h$ ; we say that  $g$  s-reduces to  $h$  via  $F$  in this case. If  $h$  cannot be further s-reduced via  $F$ , then we call it a final s-reductum of  $g$ .

It is obvious that if  $g \xrightarrow{F} h$ , then  $g - h \in R[F]$ . Well-ordering of  $\mathbf{T}_X$  implies that any chain of 1-step s-reductions must terminate.

To s-reduce  $g \in R[X]$  via a finite set  $F$  requires us to do two things at each step. After we have chosen the term  $cX^{\vec{\beta}}$  of  $g$  that we wish to eliminate, we must be able to tell

1. whether  $X^{\vec{\beta}}$  lies in the multiplicative monoid generated by  $\text{Lp}F$ , and
2. whether  $c$  belongs to the ideal of  $R$  generated by  $\{\text{lc}(F^{\vec{e}}) : \text{lp}(F^{\vec{e}}) = X^{\vec{\beta}}\}$ .

To address the first issue, we need to solve for  $\vec{e} \in \oplus_F \mathbf{N}$  in the inhomogeneous linear diophantine system arising from the exponents of the variables in the equation  $X^{\vec{\beta}} = \text{lp}(F^{\vec{e}})^{\dagger}$ . To address the second point simply requires that we determine ideal membership in  $R$ , which we have assumed is possible<sup>†</sup>.

By a standard proof, we can also show

<sup>†</sup> Refer to Dachselt (1990) for a subroutine that can determine such solutions.

<sup>‡</sup> Examples of s-reduction may be found in Miller (1994).

PROPOSITION 3.3. *The following are equivalent for  $F \subseteq A$ :*

1.  *$F$  is a SAGBI basis for  $A$*
2. *For every  $a \neq 0 \in A$ , the final  $s$ -reductum of  $a$  via  $F$  is always 0.*
3. *Every  $a \in A$  has a SAGBI representation with respect to  $F$ , that is, a representation*

$$a = \sum_{i=1}^N r_i F^{\vec{e}_i}, \quad r_i \in R$$

*such that  $\max_i \text{lp}(F^{\vec{e}_i}) = \text{lp}(a)$  (i.e.,  $\text{ht}(\sum_{i=1}^N r_i F^{\vec{e}_i}) = \text{lp}(a)$ ).*

COROLLARY 3.4. *A SAGBI basis for  $A$  generates  $A$  as an  $R$ -subalgebra .*

COROLLARY 3.5. *Suppose  $F$  is a SAGBI basis for  $A$ . An element  $p \in R[X]$  belongs to  $A$  if and only if  $p \xrightarrow{F} 0$ .*

Now we write  $A = R[F]$ , where  $F = \{f_1, f_2, \dots\}$  is not necessarily finite. To design an algorithm for constructing a SAGBI basis for  $A$ , we intend to determine a collection of polynomials related to  $F$  such that if each of these polynomials  $s$ -reduces to 0 via  $F$ , then  $F$  is a SAGBI basis. These polynomials mimic the  $S$ -polynomials of ordinary Gröbner basis theory, and this desired property will be the basis of our construction algorithm.

Represent  $A = R[F]$  as the homomorphic image of a polynomial ring  $R[Y]$  (where the cardinality of  $Y = \{y_1, y_2, \dots\}$  is the same as that of  $F$ ) via the usual evaluation homomorphism sending each  $y_i \mapsto f_i$ . We will now equip  $R[Y]$  with a graded  $R$ -module structure (which may not be based on any term order on  $R[Y]$ ). Given  $P(Y) \in R[Y]$ , we define

$$\deg P(Y) = \max\{\text{lp}(F^{\vec{a}}) : Y^{\vec{a}} \text{ occurs in } P(Y)\}.$$

<sup>†</sup>Intuitively,  $\deg P(Y)$  is the height of  $P(F)$  prior to any simplification of the latter polynomial. It is easy to check that this degree map from  $R[Y] \rightarrow \mathbf{T}_X$  truly does give a grading on  $R[Y]$ . Notice that the homogeneous elements with respect to this presumed grading will be those polynomials  $P(Y)$  whose terms give rise to  $F$ -monomials all having the same leading  $X$ -power product.

Now define an evaluation map  $\pi : R[Y] \rightarrow R[\text{Lt}F]$  via  $y_i \mapsto \text{lt}(f_i)$ . The ideal  $I(\text{Lt}F) = \{P(Y) : \pi(P(Y)) = P(\text{Lt}F) = 0\} = \ker \pi$ , which we shall refer to as the ideal of relations of  $\text{Lt}F$ , is homogeneous with respect to the  $\mathbf{T}_X$ -grading on  $R[Y]$ . Its homogeneous generators will take the place in our current theory of the usual  $S$ -polynomials. Recall that such generators may be computed using the familiar tag variable technique of ordinary Gröbner basis theory.

We are now in a position to state and prove the main result of this section.

THEOREM 3.6. *Let  $F \subseteq R[X]$ , and let  $\{P_j(Y) : j \in J\}$  be a set of  $\mathbf{T}_X$ -homogeneous generators for  $I(\text{Lt}F) \subseteq R[Y]$ .  $F$  is a SAGBI basis for  $R[F]$  if and only if for each  $j \in J$ ,  $P_j(F) \xrightarrow{F} 0$ .*

<sup>†</sup> It is not necessarily true that  $\deg P(Y) = \text{lp}(P(F))$ : for example, if  $F = \{f_1, f_2\} = \{x^2, x^2 + 1\} \subseteq R[x]$ , then  $\deg(y_2 - y_1) = x^2$ , whereas  $\text{lp}(f_2 - f_1) = 1$ .

**Proof.**  $\Rightarrow$ : This direction is a trivial corollary of Proposition 3.3.

$\Leftarrow$ : Let  $h \in R[F]$ . We will show that  $\text{lt}(h) = \sum_i r_i \text{lt}(F^{\vec{e}_i}) \in R[\text{Lt}F]$ .

Write  $h = \sum_{i=1}^m c_i F^{\vec{e}_i}$ ; furthermore, assume that this representation has the smallest possible height  $t_0 = \max_i \text{lp}(F^{\vec{e}_i})$  of all such representations. We know that  $\text{lp}(h) \leq t_0$ . Suppose that  $\text{lp}(h) < t_0$ ; without loss of generality, let the first  $N$  summands be the ones for which  $\text{lp}(F^{\vec{e}_i}) = t_0$ . Then cancellation of their leading  $X$ -power products must occur; i.e.  $\sum_{i=1}^N c_i \text{lt}(F^{\vec{e}_i}) = 0$ . Hence, we obtain an element  $P(Y) = \sum_{i=1}^N c_i Y^{\vec{e}_i} \in I(\text{Lt}F)$ . We can then write

$$\sum_{i=1}^N c_i Y^{\vec{e}_i} = P(Y) = \sum_{j=1}^M g_j(Y) P_j(Y) \quad (3.1)$$

where the elements  $P_j(Y)$  are among the stated generators of  $I(\text{Lt}F)$  and the polynomials  $g_j(Y) \in R[Y]$ . Moreover, by homogeneity of  $P(Y)$  and each  $P_j(Y)$ , we may assume that each  $g_j(Y)$  is  $\mathbf{T}_X$ -homogeneous and that  $\deg[g_j(Y)P_j(Y)] = \deg P(Y) = t_0$  for all  $j$ .

We have assumed that each  $P_j(F) \xrightarrow{F} 0$ ; therefore, we have SAGBI representations  $P_j(F) = \sum_{k=1}^{n_j} c_{kj} F^{\vec{e}_{kj}}$ . By definition, these sums must have heights  $\max_k \text{lp}(F^{\vec{e}_{kj}}) = \text{lp}(P_j(F)) < \deg P_j(Y)$  for each  $j$ , where the last inequality holds because  $P_j(Y) \in I(\text{Lt}F)$ , so that the highest  $X$ -terms in  $P_j(F)$  cancel. Then for each  $j$ ,  $1 \leq j \leq M$ ,

$$g_j(F)P_j(F) = \sum_{k=1}^{n_j} c_{kj} g_j(F) F^{\vec{e}_{kj}} \quad (3.2)$$

Define  $t_j$  to be the height of the right-hand sum in Equation (3.2), and observe that

$$t_j \leq \deg g_j(Y) \cdot \max_k \text{lp}(F^{\vec{e}_{kj}}) < \deg g_j(Y) \cdot \deg P_j(Y) = t_0.$$

Now Equations (3.1) and (3.2) imply that

$$h = P(F) + \sum_{i=N+1}^m c_i F^{\vec{e}_i} = \sum_{j=1}^M \left( \sum_{k=1}^{n_j} c_{kj} g_j(F) F^{\vec{e}_{kj}} \right) + \sum_{i=N+1}^m c_i F^{\vec{e}_i}.$$

If we examine the right-hand expression closely, we see that its height is strictly less than that of our initial representation for  $h$ , for the height of the first, double sum is the maximum of the  $t_j$  we worked with above, which is strictly less than  $t_0$ , and the height of the second, single sum is strictly less than the old maximum,  $t_0$ , by choice of  $N$ . But this contradicts our initial assumption that we had chosen a representation for  $h$  that had the smallest possible height. Thus,  $F$  is a SAGBI basis for  $R[F]$ .  $\square$

We may now present an algorithm for computing SAGBI bases. See Algorithm 3.1.

Theoretically, Algorithm 3.1 can be used with an infinite input set  $F$  because all our results so far have been carefully designed not to require any finiteness conditions. Thus, if we assume that we can find generators for  $I(\text{Lt}F)$  when  $F$  is infinite (which may be quite a stretch of imagination!), we shall see that it makes sense to apply the algorithm to any size input set. To this end, we validate that the algorithm produces a SAGBI basis, although it need not terminate, even with finite input. See Robbiano and Sweedler (1988) for a discussion of infinite SAGBI bases in  $k[X]$ .

**INPUT:**  $F$

**OUTPUT:** A SAGBI basis for  $R[F]$

**INITIALIZATION:**  $H := F$ ,  $oldH := \emptyset$

**WHILE**  $H \neq oldH$  **DO**

$Y := \{y_i : h_i \in H\}$ , a set of variables

Compute a  $\mathbf{T}_X$ -homog. generating set  $\mathcal{P}$  for  $I(\text{Lt}H)$  in  $R[Y]$ .

$red\mathcal{P} := \{\text{final s-reducta via } H \text{ of } P(H) : P(Y) \in \mathcal{P}\} - \{0\}$

$oldH := H$

$H := H \cup red\mathcal{P}$

ALGORITHM 3.1. : SAGBI Basis Construction Algorithm

**PROPOSITION 3.7.** *Let  $H_\infty = \cup H$  over all passes of the WHILE loop. Then  $H_\infty$  is a SAGBI basis for  $R[F]$ . Moreover, if  $F$  is finite and  $R[F]$  has a finite SAGBI basis, then Algorithm 3.1 terminates and produces a finite SAGBI basis for  $R[F]$ .*

**Proof.** Set  $\mathcal{P}_\infty = \cup \mathcal{P}$  over all passes of the loop, and let  $Y_\infty$  be a set of variables  $y_i$ , one for each element  $h_i \in H_\infty$ . We will show that  $\mathcal{P}_\infty$  is a set of  $\mathbf{T}_X$ -homogeneous generators for  $I(\text{Lt}H_\infty) \subseteq R[Y_\infty]$ , and then that each element of  $\mathcal{P}_\infty$  s-reduces to 0 via  $H_\infty$ .

$\mathcal{P}_\infty$  is  $\mathbf{T}_X$ -homogeneous since each  $\mathcal{P}$  of each loop is. Now choose  $P(Y_\infty) \in I(\text{Lt}H_\infty)$ . Since only finitely many  $y_i$  can occur in  $P(Y_\infty)$ , only finitely many  $h_i \in H_\infty$  occur in  $P(H_\infty)$ . The sets  $H$  are nested, so these particular  $h_i$ 's must all belong to the set  $H = H_{N_0}$  produced by the end of some finite number  $N_0$  of loops. Let  $Y_{N_0} \subseteq Y_\infty$  be the subset of variables corresponding to  $H_{N_0}$ . Then  $P(Y_\infty) \in I(\text{Lt}H_{N_0}) \subseteq \langle \mathcal{P}_\infty \rangle$ , the ideal generated by  $\mathcal{P}_\infty$  in  $R[Y_\infty]$ . Hence,  $I(\text{Lt}H_\infty) \subseteq \langle \mathcal{P}_\infty \rangle$ . Conversely, each element  $P(Y_\infty)$  of  $\mathcal{P}_\infty$  belongs to the set  $\mathcal{P}_{N_0}$  of some pass of the WHILE loop; whence,  $P(Y_\infty) \in I(\text{Lt}H_{N_0}) \subseteq I(\text{Lt}H_\infty)$ . Thus,  $\mathcal{P}_\infty \subseteq I(\text{Lt}H_\infty)$ , and  $\langle \mathcal{P}_\infty \rangle = I(\text{Lt}H_\infty)$ .

We have just pointed out that if  $P(Y_\infty) \in \mathcal{P}_\infty$ , then we may assume that  $P(Y_\infty) \in I(\text{Lt}H_{N_0})$  for some pass, in this case the  $N_0$ -th, of the loop. Clearly,  $P(Y_\infty) \rightarrow 0$  via either  $H_{N_0}$  or  $H_{N_0+1}$ ; in either case, we have  $P(Y_\infty) \rightarrow 0$  via  $H_\infty$ . Thus, by Theorem 3.6,  $H_\infty$  is a SAGBI basis for  $R[H_\infty] = R[F]$ .

Now suppose that  $R[F]$  has a finite SAGBI basis  $S$ . Because  $H_\infty$  is also a SAGBI basis, we have an expression for each  $s \in S$ :

$$\text{lt}(s) = \sum_{j=1}^{M_s} r_{j,s} \text{lt}(H_{\infty}^{\vec{e}_{j,s}}), \quad r_{j,s} \in R.$$

The finite set  $\tilde{H}$  of those elements of  $H_\infty$  for which the corresponding coordinate of some  $\vec{e}_{j,s}$  is non-zero is a SAGBI basis as well since  $R[\text{Lt}\tilde{H}] = R[\text{Lt}S] = R[\text{Lt}R[F]]$ . The set  $\tilde{H}$  must be a subset of the set  $H = H_{N_0}$  produced at the end of some finite number  $N_0$  of loops, so that  $H_{N_0}$  is also a SAGBI basis for  $R[F]$ , and by Theorem 3.6, we know that the algorithm will terminate after the next loop.

It remains to show that  $H_{N_0}$  is finite. Any loop that begins with a finite input set (as does the very first loop, by assumption on  $F$ ) will create a finite associated variable set  $Y$ . Then the Hilbert Basis Theorem applies to  $R[Y]$  to prove that we can choose the generating set  $\mathcal{P}$  of the ideal  $I(\text{Lt}H)$  to be finite as well. Hence, the output of that pass of the loop must be finite. Thus, beginning with a finite set  $F$ , Algorithm 3.1 completes a strictly finite number of loops, each of which yields finite output, and we conclude that  $H_{N_0}$  is indeed a finite SAGBI basis for  $R[F]$ .  $\square$

EXAMPLE 3.8. In this example we will compute a SAGBI basis for  $\mathbf{Z}[F] \subseteq \mathbf{Z}[x, y]$  where

$$F = \{f_1 = 4x^2y^2 + 2xy^3 + 3xy, \quad f_2 = 2x^2 + xy, \quad f_3 = 2y^2\}.$$

We use the term order degree lex with  $x > y$ .

Set  $H = F$ . It is evident that the ideal of relations  $I(\text{Lt}H) = I(4x^2y^2, 2x^2, 2y^2) \subseteq \mathbf{Z}[Y_1, Y_2, Y_3]$  is generated by  $P(Y) = Y_1 - Y_2Y_3$ . The polynomial  $P(H) = 3xy$  cannot be s-reduced via  $H$ , so that  $\text{red}\mathcal{P} = \{3xy\}$ . This forces a second pass through the WHILE loop with an additional member  $f_4 = 3xy \in H^\dagger$ .

On the second pass through the WHILE loop, we calculate generators for the new ideal  $I(\text{Lt}H) \subseteq \mathbf{Z}[Y_1, Y_2, Y_3, Y_4]$ , obtaining the set

$$\mathcal{P} = \{P_1 = Y_1 - Y_2Y_3, \quad P_2 = 9Y_1 - 4Y_4^2, \quad P_3 = 9Y_2Y_3 - 4Y_4^2\}.$$

One can check that  $P_j(H) \xrightarrow{H} 0$  for  $j = 1, 2, 3$ . Thus, the set  $\text{red}\mathcal{P}$  is empty, terminating the algorithm. Our SAGBI basis is  $\{4x^2y^2 + 2xy^3 + 3xy, 2x^2 + xy, 2y^2, 3xy\}$ .  $\triangle$

#### 4. SAGBI-Gröbner Bases in $R[X]$

We next address the topic of SAGBI-Gröbner bases in  $R[X]$  and begin by defining the primary objects of study. Then we present an algorithm for their construction. As always,  $A$  is an  $R$ -subalgebra of  $R[X]$ . The ideal of  $A$  generated by a subset  $S$  will be denoted by  $\langle S \rangle_A$ , or just  $\langle S \rangle$  when  $A$  is obvious. We will also use this notation to represent monoid-ideals of a multiplicative monoid.

DEFINITION 4.1. Let  $I \subseteq A$  be an ideal of  $A$ . A subset  $G \subseteq I$  is a SAGBI-Gröbner basis (SG-basis) for  $I$  if  $\text{Lt}G$  generates  $\langle \text{Lt}I \rangle$  in  $R[\text{Lt}A]$ .

Recall that in ordinary Gröbner basis theory every ideal is assured to have a finite Gröbner basis, due to the Hilbert Basis Theorem. By the same reasoning, we may draw this conclusion about SG-bases for ideals of  $A$ , provided that  $A$  has a finite SAGBI basis (hence  $R[\text{Lt}A]$  is finitely generated).

$\dagger$  The reader may notice that  $f_4$  is actually an s-reductum of  $f_1$  via  $\{f_2, f_3\}$  and that we could therefore have replaced  $f_1$  by  $f_4$  initially. Such inter-reduction may well make the algorithm more efficient. However, a serious analysis of improvements is outside the scope of this exposition.

We continue by describing an appropriate reduction theory for the current context.

DEFINITION 4.2. Let  $G \subseteq A, h \in A$ . We say that  $h$  si-reduces to  $h'$  via  $G$  in one step, written  $h \xrightarrow{G}_{\text{si}} h'$ , if there exist a non-zero term  $cX^{\vec{\alpha}}$  of  $h$  and elements  $g_1, \dots, g_M \in G$  and  $a_1, \dots, a_M \in A$  for which the following hold:

1.  $X^{\vec{\alpha}} = \text{lp}(a_i g_i)$  for each  $i$ .
2.  $cX^{\vec{\alpha}} = \sum_{i=1}^M \text{lt}(a_i g_i)$ .
3.  $h' = h - \sum_{i=1}^M a_i g_i$ .

We say that  $h$  si-reduces to  $h'$  via  $G$  and again write  $h \xrightarrow{G}_{\text{si}} h'$  if there is a chain of one-step si-reductions as above leading from  $h$  to  $h'$ . If  $h'$  cannot be si-reduced via  $G$ , we call it a final si-reductum of  $h$ .

We point out that  $h \xrightarrow{G}_{\text{si}} h'$  implies that  $h - h' \in \langle G \rangle_A$ . Again, well-ordering of  $\mathbf{T}_X$  implies that every  $h \in A$  must have a final si-reductum via a subset  $G$ ; that is, si-reduction terminates independent of the choices made during each single step.

To perform si-reduction, with a given term  $cX^{\vec{\alpha}}$  of  $h$ , we must determine

1. whether  $X^{\vec{\alpha}} = \text{lp}(g)\text{lp}(a)$  for some  $a \in A$  and  $g \in G$ ; that is, whether  $X^{\vec{\alpha}}$  belongs to the monoid-ideal  $\langle \text{lp}(g) \rangle_{\text{lp}A}$ , and
2. whether  $c$  can be expressed as an  $R$ -linear combination of those  $\text{lc}(ag)$ 's for which  $X^{\vec{\alpha}} = \text{lp}(ag) \in \langle \text{lp}(g) \rangle_{\text{lp}A}$ , whence Condition 2 of Definition 4.2 is satisfied.

Given a SAGBI basis  $F$  for  $A$ , answering the monoid-ideal membership question posed above amounts to searching for solutions  $\vec{\eta} \in \oplus_F \mathbf{N}$  to the equation

$$X^{\vec{\alpha}} = \text{lp}(g)\text{lp}(F^{\vec{\eta}})$$

for each  $g \in G$ ; this equation may be converted to an inhomogeneous linear diophantine system in its exponents. We can then check the desired property for the coefficient  $c$  by our assumption that ideal membership in  $R$  can be determined<sup>†</sup>.

The proofs of the next result and its corollaries again proceed in the standard way and are therefore omitted.

PROPOSITION 4.3. *The following are equivalent for a subset  $G$  of an ideal  $I \subseteq A$ :*

1.  $G$  is an SG-basis for  $I$ .
2. For every  $h \in I$ , every final si-reductum of  $h$  via  $G$  is 0.
3. Every  $h \in I$  has an SG-representation with respect to  $G$ , that is, a representation

$$h = \sum_{i=1}^M a_i g_i, \quad a_i \in A, g_i \in G$$

such that  $\max_i \text{lp}(a_i g_i) = \text{lp}(h)$  (i.e.,  $\text{ht}(\sum_{i=1}^M a_i g_i) = \text{lp}(h)$ ).

COROLLARY 4.4. *An SG-basis for  $I$  generates  $I$  as an ideal of  $A$ .*

<sup>†</sup> Again, examples may be found in Miller (1994).



COROLLARY 4.5. *Suppose that  $G$  is an SG-basis for  $I \subseteq A$ . Then  $a \in A$  belongs to  $I$  if and only if  $a \xrightarrow{G}_{\text{si}} 0$ .*

We introduce some basic concepts and notation.

DEFINITION 4.6. For an  $R$ -subalgebra  $A \subseteq R[X]$  and a subset  $S \subseteq A$ ,

1.  $\text{Syz}_A(S) = \{\vec{a} = (a_s)_{s \in S} \in \oplus_S A : \sum_{s \in S} a_s s = 0\}$ , the  $A$ -module of syzygies of  $S$  whose coordinates all belong to  $A$ . We call an element of  $\text{Syz}_A(S)$  an  $A$ -syzygy of  $S$ . (We will omit the subscript when the subalgebra  $A$  is obvious.)
2. An element  $\vec{a} = (a_s)_{s \in S} \in \text{Syz}_A(S)$  is homogeneous of degree  $X^{\vec{a}}$  if  $\text{lp}(a_s)\text{lp}(s) = X^{\vec{a}}$  for each  $a_s s \neq 0$ ; we denote this by writing  $\deg(\vec{a}) = X^{\vec{a}}$ .
3. For  $\vec{a} = (a_s)_{s \in S} \in \oplus_S A$ , let  $\vec{\text{lt}}(\vec{a})$  represent the vector  $(\text{lt}(a_s))_{s \in S}$ .

DEFINITION 4.7. We call a subset  $\mathcal{Q} \subseteq \oplus_S A$  an lt-generating set for  $\text{Syz}(\text{Lt}S)$  if  $\{\vec{\text{lt}}(\vec{Q}) : \vec{Q} \in \mathcal{Q}\}$  generates the  $R[\text{Lt}A]$ -module  $\text{Syz}_{R[\text{Lt}A]}(\text{Lt}S)$ . Furthermore, we call such a set  $\mathcal{Q}$  homogeneous if each of the vectors  $\vec{\text{lt}}(\vec{Q})$  is homogeneous as a syzygy of  $\text{Lt}S$ .

For the remainder of this section we assume that  $A$  has a finite SAGBI basis, and that  $G = \{g_1, \dots, g_M\} \subseteq A$  is finite as well; this assures computability. Furthermore, we will omit the subscript when discussing the  $R[\text{Lt}A]$ -module  $\text{Syz}(\text{Lt}G)$ . Given a homogeneous lt-generating set  $\mathcal{Q}$  and writing its elements as  $\vec{Q}_j = (q_{j,1}, \dots, q_{j,M})$ , we shall see that the polynomials  $\sum_{i=1}^M q_{j,i} g_i$  take the place in our present setting of S-polynomials.

THEOREM 4.8. *Let  $G = \{g_1, \dots, g_M\} \subseteq A$ ; let  $\mathcal{Q}$  be a homogeneous lt-generating set for  $\text{Syz}(\text{Lt}G)$ . Then  $G$  is an SG-basis for  $\langle G \rangle_A$  if and only if for each  $\vec{Q}_j = (q_{j,1}, \dots, q_{j,M}) \in \mathcal{Q}$ , we have  $\sum_{i=1}^M q_{j,i} g_i \xrightarrow{G}_{\text{si}} 0$ .*

**Proof.**  $\Rightarrow$ : The result is a direct consequence of Proposition 4.3.

$\Leftarrow$ : Let  $h \in \langle G \rangle_A$ ; we intend to show that  $\text{lt}(h) \in \langle \text{Lt}G \rangle_{R[\text{Lt}A]}$ . Write  $h = \sum_{i=1}^m a_i g_i$  such that the height  $t_0 = \max_i \text{lp}(a_i g_i)$  of this representation is minimal with respect to all such representations for  $h$ . Now  $\text{lp}(h) \leq t_0$ ; suppose that  $\text{lp}(h) < t_0$ . Without loss of generality, assume that our representation is written such that  $a_1 g_1, \dots, a_{M_0} g_{M_0}$  contribute to the height, in the sense of Definition 2.3. Setting  $\vec{a}' = (a_1, \dots, a_{M_0}, 0, \dots, 0)$ , we see that  $\vec{\text{lt}}(\vec{a}') \in \text{Syz}(\text{Lt}G)$  and is homogeneous. Thus, there exist  $b_1, \dots, b_N \in A$  and  $\vec{Q}_1, \dots, \vec{Q}_N \in \mathcal{Q}$  such that  $\vec{\text{lt}}(\vec{a}') = \sum_{j=1}^N \text{lt}(b_j) \vec{\text{lt}}(\vec{Q}_j)$ ; also, we may assume that  $\deg(\text{lt}(b_j) \vec{\text{lt}}(\vec{Q}_j)) = \deg(\vec{\text{lt}}(\vec{a}')) = t_0$  for all  $j$  by homogeneity of the syzygies involved. Moreover, because every non-zero  $\text{lt}(b_j) \text{lt}(q_{j,i}) \text{lt}(g_i) = \deg(\text{lt}(b_j) \vec{\text{lt}}(\vec{Q}_j)) = t_0$ , the elements  $b_j$  and  $\vec{Q}_j$  may be chosen so that the expression  $\sum_{j=1}^N \text{lt}(b_j) \text{lt}(q_{j,i})$  is homogeneous in  $R[X]$  for all  $i$ .

Now

$$h = \sum_{i=1}^M a_i g_i - \sum_{i=1}^M \left( \sum_{j=1}^N b_j q_{j,i} \right) g_i + \sum_{j=1}^N b_j \left( \sum_{i=1}^M q_{j,i} g_i \right)$$

$$= \sum_{i=1}^M \left( a_i - \sum_{j=1}^N b_j q_{j,i} \right) g_i + \sum_{j=1}^N b_j \left( \sum_{i=1}^M p_{j,i} g_i \right) \quad (4.1)$$

where  $\sum_{i=1}^M p_{j,i} g_i$  is an SG-representation for  $\sum_{i=1}^M q_{j,i} g_i$ , which exists since we have supposed that every  $\sum_{i=1}^M q_{j,i} g_i \xrightarrow{G}_{\text{si}} 0$ . Furthermore, if we define  $t_j = \text{ht}(\sum_{i=1}^M p_{j,i} g_i)$ , then we have

$$t_j = \text{lp} \left( \sum_{i=1}^M q_{j,i} g_i \right) < \max_i \text{lp}(q_{j,i} g_i) \quad \text{for all } j,$$

where the inequality holds because  $\vec{\text{lt}}(\vec{Q}_j) \in \text{Syz}(\text{Lt}G)$ .

We proceed to show that the representation for  $h$  in Equation (4.1) has lesser height than our original representation. Consider the first sum, in which the coefficient of  $g_i$  is assumed to be a simplified polynomial in  $R[X]$ . For  $i \leq M_0$ , we know that  $\text{lt}(a_i) = \text{lt}(\sum_{j=1}^N b_j q_{j,i})$  by homogeneity of  $\sum_{j=1}^N b_j q_{j,i}$  in  $R[X]$ ; therefore, due to cancellation of the highest terms,  $\text{lp}[(a_i - \sum_{j=1}^N b_j q_{j,i}) g_i] < \text{lp}(a_i g_i) = t_0$ , our original height. For  $i > M_0$ ,  $\text{lp}(a_i g_i) < t_0$  and also  $\sum_{j=1}^N \text{lt}(b_j) \text{lt}(q_{j,i}) = 0$ , which implies that

$$\text{lp} \left( \sum_{j=1}^N b_j q_{j,i} g_i \right) < \max_j \text{lp}(b_j q_{j,i} g_i) = \deg(\text{lt}(b_j) \vec{\text{lt}}(\vec{Q}_j)) = t_0.$$

Since  $\text{lp}[(a_i - \sum_{j=1}^N b_j q_{j,i}) g_i] \leq \max\{\text{lp}(a_i g_i), \text{lp}(\sum_{j=1}^N b_j q_{j,i} g_i)\} < t_0$  for all  $i$ , the height of the first sum in Equation (4.1) must be less than  $t_0$ .

Now for the second sum in Equation 4.1, we have the following:

$$\begin{aligned} \text{ht} \left( \sum_{j=1}^N b_j \sum_{i=1}^M p_{j,i} g_i \right) &\leq \max_{i,j} \text{lp}(b_j p_{j,i} g_i) = \max_j [\text{lp}(b_j) \cdot t_j] \\ &< \max_{i,j} \text{lp}(b_j q_{j,i} g_i) = \deg(\vec{\text{lt}}(\vec{a}')) = t_0 \end{aligned}$$

Hence, Equation (4.1) does provide a new representation for  $h \in \langle G \rangle_A$  having smaller height than our assumed minimum. Therefore,  $\text{lp}(h) = t_0$ , so that  $\text{lt}(h) = \sum_{i=1}^{M_0} \text{lt}(a_i g_i) \in \langle \text{Lt}G \rangle$ , proving that  $G$  is an SG-basis for  $\langle G \rangle_A$ .  $\square$

We next describe how an  $\text{lt}$ -generating set for  $\text{Syz}(\text{Lt}G)$  may be computed (when  $G = \{g_1, \dots, g_M\}$  is finite). The method is based on the following result, whose proof is straight-forward.

**PROPOSITION 4.9.** *Let  $\pi : \mathcal{R} \rightarrow \mathcal{S}$  be a ring epimorphism. Let  $S' = \{s_1, \dots, s_M\} \subseteq \mathcal{S}$  be given, and choose a set  $\bar{S}' = \{\bar{s}_1, \dots, \bar{s}_M\}$  of pre-images in  $\mathcal{R}$ . Suppose that  $\vec{P}_1, \dots, \vec{P}_L \in \mathcal{R}^M$  with  $\vec{P}_j = (p_{j,1}, \dots, p_{j,M})$  are such that*

$$\vec{P}_1, \dots, \vec{P}_K \text{ generate } \text{Syz}(\bar{s}_1, \dots, \bar{s}_M) \subseteq \mathcal{R}^M$$

*while for the remaining  $\{\vec{P}_{K+1}, \dots, \vec{P}_L\}$ ,*

$$\sum_{i=1}^M p_{K+1,i} \bar{s}_i, \dots, \sum_{i=1}^M p_{L,i} \bar{s}_i \text{ generate } \ker(\pi) \cap \langle \bar{s}_1, \dots, \bar{s}_M \rangle \subseteq \mathcal{R}.$$

Then  $\text{Syz}(s_1, \dots, s_M)$  is generated by the set  $\{\vec{\pi}(\vec{P}_1), \dots, \vec{\pi}(\vec{P}_L)\}$ , where we define  $\vec{\pi} : \mathcal{R}^M \longrightarrow \mathcal{S}^M$  via  $\vec{\pi}(r_1, \dots, r_M) = (\pi(r_1), \dots, \pi(r_M))$  for  $r_1, \dots, r_M \in \mathcal{R}$ .

To apply this result to a finite subset  $G \subseteq A$ , we take  $\mathcal{S} = R[\text{Lt}A] = R[\text{Lt}F]$  where  $F$  is a finite SAGBI basis for  $A$ , set  $\mathcal{R} = R[Y]$  where  $Y$  is a set of variables of the same cardinality as  $F$ , and take  $\pi$  to be the obvious evaluation map. Proposition 4.9 (with  $S' = \text{Lt}G$ ) and ordinary Gröbner basis techniques then allow us to compute generators for  $\text{Syz}(\text{Lt}G)$ , from which we may obtain a homogeneous generating set  $\mathcal{P} = \{\vec{P}_1, \dots, \vec{P}_N\}$  for  $\text{Syz}(\text{Lt}G)$ . Furthermore, we may choose  $\mathcal{P}$  so that for each generator  $\vec{P}_j(\text{Lt}F) = (P_{j,1}(\text{Lt}F), \dots, P_{j,M}(\text{Lt}F))$ , the polynomials  $P_{j,i}(\text{Lt}F)$  are homogeneous in  $R[X]$ . Defining

$$\widetilde{P_{j,i}}(F) = \begin{cases} P_{j,i}(F) & \text{if } P_{j,i}(\text{Lt}F) \neq 0 \\ 0 & \text{otherwise,} \end{cases}$$

we see that the set  $\mathcal{Q} = \{\vec{Q}_j = (\widetilde{P_{j,1}}(F), \dots, \widetilde{P_{j,M}}(F)) : j = 1, \dots, N\}$  is a homogeneous lt-generating set for  $\text{Syz}(\text{Lt}G)$  since  $\text{lt}(\vec{Q}_j) = \vec{P}_j(\text{Lt}F)$  for all  $j$ <sup>†</sup>.

Next we present an algorithm for computing SG-bases. See Algorithm 4.1.

**INPUT:** A finite set  $G \subseteq A$ , a finite SAGBI basis  $F$  for  $A$

**OUTPUT:** An SG-basis  $H$  for  $\langle G \rangle_A$

**INITIALIZATION:**  $H := G$ ,  $oldH := \emptyset$

**WHILE**  $H \neq oldH$  **DO**

Compute a homogeneous lt-generating set  $\mathcal{Q}$  for  $\text{Syz}(\text{Lt}H)$ .

$\mathcal{P} := \{\sum_{h \in H} q_h h : (q_h)_{h \in H} \in \mathcal{Q}\}$

$red\mathcal{P} := \{\text{final si-reducta via } H \text{ of each element of } \mathcal{P}\} - \{0\}$

$oldH := H$

$H := H \cup red\mathcal{P}$

ALGORITHM 4.1. : SG-Basis Construction Algorithm

**PROPOSITION 4.10.** *Algorithm 4.1 yields a finite SG-basis for  $\langle G \rangle_A$  (when  $G$  is finite and  $A$  has a finite SAGBI basis).*

<sup>†</sup> This construction of the elements  $\widetilde{P_{j,i}}(F)$  is necessary since  $P_{j,i}(\text{Lt}F) = 0$  need not imply that  $P_{j,i}(F) = 0$ , whence  $\text{lt}(\vec{Q}_j)$  need not be a homogeneous syzygy of  $\text{Lt}G$ .

**Proof.** We first show that the algorithm produces an SG-basis, then that the resulting basis is finite.

Let  $H_i$  denote the current set  $H$  at the beginning of the  $i$ -th pass of the WHILE loop. Then the ideals generated in  $R[\text{Lt}A]$  by each successive set  $\text{Lt}H_i$  form a nested, non-decreasing sequence. Since  $A$  has a finite SAGBI basis, the Hilbert Basis Theorem applies to  $R[\text{Lt}A]$ , as noted earlier; therefore the chain of ideals stabilizes at some point with  $\langle \text{Lt}H_{N_0-1} \rangle = \langle \text{Lt}H_{N_0} \rangle = \dots$ . The algorithm will then terminate during the  $N_0$ -th pass of the loop since the set  $\text{Syz}(\text{Lt}H)$  will not have changed since the previous pass and thus the same set  $\mathcal{Q}$  may be chosen. Clearly,  $\text{red}\mathcal{P}$  will then be empty, and, by Theorem 4.8, the resulting output  $H_{N_0}$  will be an SG-basis for  $\langle G \rangle_A$ .

We will now show that  $H_{N_0}$  is finite. Our technique for computing an lt-generating set for  $\text{Syz}(\text{Lt}H)$  involved calculating a homogeneous generating set for  $\text{Syz}(\text{Lt}H)$ ; according to Definition 4.7, these two generating sets obviously have the same cardinality. Since  $R[\text{Lt}A]$  is noetherian, we may choose a finite generating set for  $\text{Syz}(\text{Lt}H)$  when the input set  $H$  for the loop is finite. Therefore,  $\mathcal{P}$  and consequently the output of such a loop are finite. Then  $H_{N_0}$ , as the result of a finite number of passes of the loop beginning with finite input  $G$ , is a finite SG-basis for  $\langle G \rangle_A$ .  $\square$

The example below demonstrates how to compute an SG-basis.

EXAMPLE 4.11. We take  $A = \mathbf{Z}[F] \subseteq \mathbf{Z}[x, y]$  where

$$F = \{f_1 = 2x^2 + xy, \quad f_2 = 2y^2, \quad f_3 = 3xy\},$$

and let  $G \subseteq \mathbf{Z}[F]$  be given by

$$G = \{g_1 = f_1 f_2 = 4x^2 y^2 + 2xy^3, \quad g_2 = f_2 f_3^2 = 18x^2 y^4\}.$$

We will again use the term order degree lex with  $x > y$ , with respect to which we have already found in Example 3.8 that  $F$  is a SAGBI basis for  $A^\dagger$ .

We begin by setting  $H = G$ . Applying the technique described after Proposition 4.9, we calculate a homogeneous lt-generating set  $\mathcal{Q} = \{(f_3^2, -f_1), (9f_2, -4)\}$  for  $\text{Syz}(\text{Lt}H)^\ddagger$ ; we obtain the associated set  $\mathcal{P} = \{0, 36xy^5\}$ . We easily see that  $\text{red}\mathcal{P} = \{36xy^5\}$  since this element cannot be si-reduced via  $H$ . Therefore, we define  $g_3 = 36xy^5$  and conduct a second pass of the WHILE loop. This time, we construct

$$\mathcal{Q} = \{(f_3^2, -f_1, 0), (3f_2 f_3, 0, -f_1), (0, 3f_2, -f_3), (-9f_2, 4, 0)\}.$$

This again yields  $\mathcal{P} = \{0, 36xy^5\}$ , so clearly  $\text{red}\mathcal{P} = \emptyset$  now, and the stopping criterion  $H = \text{old}H$  is satisfied. We have that  $\{4x^2 y^2 + 2xy^3, 18x^2 y^4, 36xy^5\}$  is an SG-basis for  $\langle G \rangle_A$ .  $\triangle$

## 5. A-syzygies

To conclude, we present a method for calculating a set of generators for  $\text{Syz}_A(H)$  given a finite subset  $H$  of an  $R$ -subalgebra  $A \subseteq R[X]$ , where we again assume that  $A$  has a finite SAGBI basis. Our technique is based on the following theorem:

<sup>†</sup> Actually, the output of Example 3.8 contained the redundant polynomial  $4x^2 y^2 + 2xy^3 + 3xy$ , which we now omit in order to simplify our computations.

<sup>‡</sup> Some of the intermediate computations were performed using the Mathematica sub-package GroebnerZ designed by Nakos and Glinos (1994).

**THEOREM 5.1.** *Let  $G = \{g_1, \dots, g_M\} \subseteq A$  be a finite SG-basis for  $\langle G \rangle_A$ . Let  $\mathcal{Q} = \{\vec{Q}_1, \dots, \vec{Q}_N\}$  be a homogeneous lt-generating set for  $\text{Syz}(\text{Lt}G)$ , and let each  $\vec{Q}_j = (q_{j,1}, \dots, q_{j,M})$ . For each  $j$ , let  $\sum_{i=1}^M a_{j,i}g_i$  be an SG-representation for  $\sum_{i=1}^M q_{j,i}g_i$ . Then  $\text{Syz}_A(G)$  is generated as an  $A$ -module by the vectors*

$$\vec{P}_j = (q_{j,1} - a_{j,1}, \dots, q_{j,M} - a_{j,M}), \quad j = 1, \dots, N.$$

**Proof.** Let  $\mathcal{M}$  represent the  $A$ -submodule of  $\text{Syz}_A(G)$  generated by the set  $\{\vec{P}_1, \dots, \vec{P}_N\}$ , and suppose that the conclusion of the theorem is false. Then we can choose  $\vec{h} = (h_1, \dots, h_M) \in \text{Syz}_A(G) - \mathcal{M}$ , such that  $t_0 = \text{ht}(\sum_{i=1}^M h_i g_i)$  as defined in Definition 2.3 is minimal among such elements of  $\text{Syz}_A(G)$ . Without loss of generality, we assume that precisely  $h_1, \dots, h_{M_0}$  contribute to the height of this expression. This implies that  $\sum_{i=1}^{M_0} \text{lt}(h_i) \text{lt}(g_i) = 0$ , i.e., that  $\vec{\text{lt}}(\vec{h}')$  is a homogeneous member of  $\text{Syz}(\text{Lt}G)$  where  $\vec{h}' = (h_1, \dots, h_{M_0}, 0, \dots, 0)$ . Therefore, we can write

$$\vec{\text{lt}}(\vec{h}') = \sum_{j=1}^N \text{lt}(b_j) \vec{\text{lt}}(\vec{Q}_j) \quad (5.1)$$

where  $\deg[\text{lt}(b_j) \vec{\text{lt}}(\vec{Q}_j)] = \deg(\vec{\text{lt}}(\vec{h}')) = t_0$  for all  $j$  such that  $b_j \neq 0$ . Also, as we saw in the proof of Theorem 4.8, we may assume that the expression  $\sum_{j=1}^N \text{lt}(b_j) \text{lt}(q_{j,i})$  is homogeneous in  $R[X]$  for all  $i$ .

Let us now consider the element  $\vec{s} = \vec{h} - \sum_{j=1}^N b_j \vec{P}_j \in \text{Syz}_A(G) - \mathcal{M}$ . We claim that  $\text{ht}(\sum_{i=1}^M s_i g_i) < \text{ht}(\sum_{i=1}^M h_i g_i)$ , where  $s_i$  represents the  $i$ -th coordinate of  $\vec{s}$ . It is important to note that  $s_i$  is the simplified form of  $h_i - \sum_{j=1}^N b_j (q_{j,i} - a_{j,i})$ . By examining certain portions of this expression for  $s_i$ , we intend to show that  $\text{lp}(s_i g_i) < t_0$  for all  $i$ .

First, we deduce that, for every  $i = 1, \dots, M$  and  $j = 1, \dots, N$ ,

$$\text{lp}(b_j a_{j,i} g_i) \leq \text{lp}\left(b_j \sum_{i=1}^M q_{j,i} g_i\right) < \text{ht}\left(b_j \sum_{i=1}^M q_{j,i} g_i\right) = \deg(\text{lt}(b_j) \vec{\text{lt}}(\vec{Q}_j)) = t_0, \quad (5.2)$$

where the first inequality follows from the definition of SG-representation and the second because  $\vec{\text{lt}}(\vec{Q}_j) \in \text{Syz}(\text{Lt}G)$ , causing the highest terms of  $b_j \sum_{i=1}^M q_{j,i} g_i$  to cancel out.

For  $i \leq M_0$ , our aim is to show that  $\text{lt}(\sum_{j=1}^N b_j (q_{j,i} - a_{j,i}) g_i) = \text{lt}(h_i g_i)$ , which equals  $c_i t_0$  for some  $c_i \in R$  since  $h_i$  contributes to  $t_0$ . Cancellation of these leading terms while condensing the expression for  $s_i g_i$  proves the claim that  $\text{lp}(s_i g_i) < t_0$ . Now Equation 5.1 and the assumption that  $i \leq M_0$  imply that  $\sum_{j=1}^N \text{lt}(b_j) \text{lt}(q_{j,i}) = \text{lt}(h_i)$ , which is non-zero (since  $h_i$  contributes to  $t_0$ ). The homogeneity and non-vanishing of this sum guarantee that the highest terms in  $\sum_{j=1}^N b_j q_{j,i} g_i$  are not eliminated. Thus,

$$\text{lt}\left(\sum_{j=1}^N b_j q_{j,i} g_i\right) = \sum_{j=1}^N \text{lt}(b_j) \text{lt}(q_{j,i}) \text{lt}(g_i) = \text{lt}(h_i g_i) = c_i t_0.$$

Recalling Inequality 5.2, we see that subtracting the sum  $\sum_{j=1}^N b_j a_{j,i} g_i$  from  $\sum_{j=1}^N b_j q_{j,i} g_i$  will not affect the leading term of the latter. Hence, we have  $\text{lt}(\sum_{j=1}^N b_j (q_{j,i} - a_{j,i}) g_i) = \text{lt}(h_i g_i)$ , as desired for  $i \leq M_0$ .

For  $i > M_0$ , we note that  $\sum_{j=1}^N \text{lt}(b_j) \text{lt}(q_{j,i}) = \text{lt}(0)$  by Equation 5.1. This identity shows that the highest terms in  $\sum_{j=1}^N b_j q_{j,i} g_i$  must cancel out, and since by homogeneity

each is a constant multiple of  $\deg(\text{lt}(b_j)\vec{\text{lt}}(\vec{Q}_j)) = t_0$ , the actual leading power product of the sum is less than  $t_0$ . We apply this inequality, Inequality 5.2, and the hypothesis that  $\text{lp}(h_i g_i) < t_0$  for  $i > M_0$  to see that

$$\text{lp}(s_i g_i) \leq \max \left\{ \text{lp}(h_i g_i), \text{lp} \left( \sum_{j=1}^N b_j q_{j,i} g_i \right), \text{lp} \left( \sum_{j=1}^N b_j a_{j,i} g_i \right) \right\} < t_0.$$

Hence,  $\text{lp}(s_i g_i) < t_0$  for all  $i$ , and we indeed have  $\max_i \text{lp}(s_i g_i) < t_0$ , which contradicts our assumption of the minimality of  $t_0$  for heights of elements of  $\text{Syz}_A(G) - \mathcal{M}$ . Therefore, this difference is empty, and  $\text{Syz}_A(G) = \mathcal{M}$ .  $\square$

The previous theorem is the appropriate generalization to our context of the corresponding result in the case where  $A = k[X]$ . Furthermore, the remainder of our discussion follows from Theorem 5.1 in an identical manner to that of the standard  $k[X]$  case, a complete description of which can be found in such texts as Adams and Loustau (1994). In fact, the proof of Theorem 3.4.3 in that reference may be carried verbatim into our current context to verify the validity of the technique below; consequently, this verification will be omitted.

We now outline a method for computing generators for the  $A$ -syzygy module  $\text{Syz}_A(H)$  of an arbitrary finite subset  $H \subseteq A$ . First, compute an SG-basis  $G$  for  $\langle H \rangle_A$  and then produce matrices  $\mathcal{W}$  and  $\mathcal{U}$  with entries in  $A$  such that  $H = \mathcal{W}G$  and  $G = \mathcal{U}H$ , where we now view  $G$  and  $H$  as column vectors<sup>†</sup>. Apply Theorem 5.1 to compute generators  $\vec{P}_1, \dots, \vec{P}_N$  for  $\text{Syz}_A(G)$ . The module  $\text{Syz}_A(H)$  is then generated by the vectors  $\vec{P}_j \mathcal{U}$  together with the row vectors of  $\mathcal{I} - \mathcal{W}\mathcal{U}$ , where  $\mathcal{I}$  is the identity matrix of the appropriate size. We conclude with an example.

EXAMPLE 5.2. Again, we take  $A = \mathbf{Z}[F] \subseteq \mathbf{Z}[x, y]$  where

$$F = \{f_1 = 2x^2 + xy, \quad f_2 = 2y^2, \quad f_3 = 3xy\}$$

is a SAGBI basis for  $A$  with respect to our term order, degree lex with  $x > y$ . Let

$$H = \{h_1 = 4x^2y^2 + 2xy^3, \quad h_2 = 10x^2y^4 + 4xy^5, \quad h_3 = 36xy^5\} \subseteq A.$$

It is apparent that the renamed SG-basis

$$G = \{g_1 = 4x^2y^2 + 2xy^3, \quad g_2 = 18x^2y^4, \quad g_3 = 36xy^5\}$$

of Example 4.11 is also an SG-basis for  $\langle H \rangle_A$ , for we observe that  $\langle G \rangle_A = \langle H \rangle_A$  since  $h_1 = g_1$ ,  $h_2 = g_2 - f_2 g_1$ , and  $h_3 = g_3$ . Thus, we have the change-of-basis matrices

$$\mathcal{W} = \begin{bmatrix} 1 & 0 & 0 \\ -f_2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \mathcal{U} = \begin{bmatrix} 1 & 0 & 0 \\ f_2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

described above. Because  $\mathcal{I} - \mathcal{W}\mathcal{U}$  is the zero-matrix, the only non-trivial generators for  $\text{Syz}_A(H)$  are the vectors  $\vec{P}_j \mathcal{U}$ , which we will now compute.

We recall the homogeneous lt-generating set

$$\mathcal{Q} = \{\vec{Q}_1 = (f_3^2, -f_1, 0), \quad \vec{Q}_2 = (3f_2 f_3, 0, -f_1), \quad \vec{Q}_3 = (0, 3f_2, -f_3), \quad \vec{Q}_4 = (-9f_2, 4, 0)\}$$

<sup>†</sup>  $\mathcal{W}$  is produced during si-reduction of the elements of  $H$  via  $G$ , and  $\mathcal{U}$  may be determined by keeping track of si-reductions during the computation of  $G$  from  $H$  by Algorithm 4.1.

for  $\text{Syz}(\text{Lt}G)$  as described at the end of Example 4.11. For the first three of these vectors, the polynomials  $\sum_{i=1}^3 q_{j,i}g_i = 0$ ; thus,  $\vec{P}_j = \vec{Q}_j$  for  $j = 1, 2, 3$ . However,  $\vec{Q}_4$  gives us the expression  $-9f_2g_1 + 4g_2 = -36xy^5 = -g_3$ , yielding  $\vec{P}_4 = (-9f_2, 4, 1)$ . We conclude that

$$\begin{aligned}\vec{P}_1\mathcal{U} &= (f_3^2 - f_1f_2, -f_1, 0), & \vec{P}_2\mathcal{U} &= (3f_2f_3, 0, -f_1), \\ \vec{P}_3\mathcal{U} &= (3f_2^2, 3f_2, -f_3), & \text{and } \vec{P}_4\mathcal{U} &= (-5f_2, 4, 1)\end{aligned}$$

generate  $\text{Syz}_A(H)$  as an  $A$ -module.  $\triangle$

### Acknowledgements

This paper is derived from my doctoral dissertation, directed by Dr. William Adams, to whom I am deeply grateful. Thanks also go to Dr. Philippe Loustau for his helpful comments, and to the referees for many illuminating suggestions.

### References

- Adams, W., Loustau, P. (1994). *An Introduction to Gröbner Bases*. American Mathematical Society, Providence.
- Becker, T., Weispfenning, V. (1993). *Gröbner Bases: A Computational Approach to Commutative Algebra*. Springer-Verlag, New York.
- Buchberger, B. (1965). *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal*. PhD. Thesis, Inst. University of Innsbruck, Innsbruck, Austria.
- Buchberger, B. (1985). Gröbner Bases: An algorithmic method in polynomial ideal theory. *Multidimensional Systems Theory* (N.K. Bose, ed.), Reidel, Dordrecht, 184-232.
- Cox, D., Little, J., O'Shea, D. (1992). *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer-Verlag, New York.
- Dachsel, T. (1990). *Ein Vervollständigungsverfahren zur Berechnung kanonischer Basen für unitäre Unterringe von Polynomringen*. Diplomarbeit, Universität Kaiserslautern.
- Kapur, D., Madlener, K. (1989). A Completion Procedure for Computing a Canonical Basis for a  $k$ -Subalgebra. *Computers and Mathematics*, Springer, New York, 1-11.
- Miller, J.L. (1994). *Algorithms for Computing in Subalgebras of Polynomial Algebras over a Ring*. Ph.D. dissertation, University of Maryland, College Park, MD.
- Möller, H.M. (1989). On the construction of Gröbner bases using syzygies. *Computational Aspects of Commutative Algebra* (L. Robbiano, ed.), Academic Press, San Diego, 211-225.
- Nakos, G., Glinos, N. (1994). Computing Gröbner Bases over  $\mathbf{Z}$ . To appear. United States Naval Academy, Annapolis, MD.
- Ollivier, F. (1990). Canonical bases: relations with standard bases, finiteness conditions and application to tame automorphisms. *Effective Methods in Algebraic Geometry* (T. Mora and C. Traverso, eds.), Birkhauser, Boston, 379-400.
- Robbiano, L. (1986). On the Theory of Graded Structures. *Journal of Symbolic Computation* **2**, 139-170.
- Robbiano, L., Sweedler, M. (1988). Subalgebra Bases. *Proc. Commutative Algebra Salvador* (W. Burns and A. Simis, eds.), Springer LNM **1430**, 61-87.
- Sweedler, M. (1988). Ideal bases and valuation rings. Manuscript. Cornell University, Ithaca, NY.
- Trinks, W. (1978). Über Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen. *J. Number Th.* **10**/4, 475-488.
- Zacharias, G. (1978). *Generalized Gröbner bases in commutative polynomial rings*. Bachelor's Thesis, MIT, Cambridge, MA.